FUGA DE INFORMACIÓN · ANÁLISIS DE DISPOSITIVOS USB

UNA MEMORIA NUEVA CADA DÍA ES UNA BANDERA; UNA TRAS OTRA, ES UN DESFILE.

EL REGISTRO QUE CASI NADIE CONOCE: CADA DISPOSITIVO QUE ALGUNA VEZ TOCÓ EL EQUIPO

> **UNA MEMORIA DE TRABAJO ENTRA Y SALE CIEN VECES; UNA MEMORIA DE SAQUEO ENTRA UNA VEZ, SE LLENA Y DESAPARECE.**

Línea de tiempo forense de la actividad del usuario, reconstruida sobre copia certificada.

EL PROBLEMA

Una empresa sospechaba que un empleado se había llevado información y encargó la pregunta clásica: ¿el equipo registra fuga, por plataformas en línea o por dispositivos de almacenamiento? Para llegar al disco hubo que desarmar el equipo —la unidad iba empotrada en la placa—, conectarlo por adaptador y generar la copia forense.

Sobre esa copia se reconstruyó la línea de tiempo completa de la actividad del usuario, buscando no solo si hubo extracción, sino cómo, cuándo y con qué preparación.

LA INTERVENCIÓN

La computadora guarda un registro que casi nadie conoce: la fecha de la primera y la última vez que cada dispositivo de almacenamiento fue conectado al equipo. Y ahí apareció la alarma, con forma de estadística: lo común es que una memoria de trabajo se use cien veces a lo largo de meses; lo que mostraba este equipo era una sucesión de dispositivos distintos conectados por primera y por última vez en los días críticos.

Ese patrón es la firma de la extracción física: no es el uso cotidiano de una memoria de trabajo, es una serie de dispositivos de un solo uso, conectados para vaciar y retirados para no volver. Los registros del sistema no dicen por sí solos qué archivos viajaron, pero sí cuándo, cuántas y con qué ritmo cambiaron las memorias — y ese ritmo era el de una mudanza, no el de una rutina.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.

EL BLOQUEO QUE NO SE AUDITA ES DECORACIÓN.

LA PREGUNTA CORRECTA NO ES «¿SE CONECTÓ ALGUNA USB?» SINO CUÁNTAS DISTINTAS, POR PRIMERA Y ÚLTIMA VEZ, EN LOS DÍAS CRÍTICOS

QUÉ SE LOGRÓ

Gracias a la línea de tiempo forense, la empresa obtuvo certeza técnica en su investigación interna: el patrón de dispositivos de un solo uso en los días críticos —antes de la salida del empleado— documentó la extracción física con precisión de calendario, aunque las memorias ya estuvieran del otro lado de la ciudad.

> **La lección para direcciones de sistemas y de recursos humanos: el registro del sistema lleva la cuenta de cada dispositivo que alguna vez tocó el equipo. Auditarlo antes de que el empleado salga por la puerta es la diferencia entre sospechar y probar.**

POR QUÉ DURIVA ES LA MEJOR OPCIÓN

≡

EFICIENCIA

Metodología propia probada en miles de dictámenes, con equipos que trabajan en paralelo sobre la evidencia.

TIEMPO

Respuesta ágil en escenarios de urgencia procesal, con la misma calidad técnica y documentación completa.

18

TRAYECTORIA

Más de 18 años de cómputo forense en México y América Latina. Creador del primer sistema operativo forense latinoamericano, presidente del Consejo Americano de Ciberseguridad y Cómputo Forense, autor de seis libros especializados.

Si un empleado salió con información, el equipo lleva el diario de cada puerta que tocó. Somos su aliado digital.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.